

EXHIBIT A



8201 GREENSBORO DRIVE, SUITE 717
MCLEAN, VA 22102
703.288.3380

425 COMMERCE DRIVE, SUITE 125
FORT WASHINGTON, PA 19034
215.646.1299

900 NORTH FRANKLIN, SUITE 608
CHICAGO, IL 60610
312.202.0715

41 EAST 11TH STREET, FLOOR 11
NEW YORK, NY 10003
212.699.3622

Brian T. Wolfinger

267-231-2135 Cellular

215-646-1299 Office

bwolfinger@ldiscovery.com

Career Summary

I have over ten years of information technology and law enforcement experience, with expertise in:

- Digital forensics;
- Information systems security;
- Network security, intrusion detection and prevention;
- Computer security incident response; and,
- Criminal investigations, interviewing, evidence gathering and general police work.

As well, I have testified in hundreds of criminal and civil cases.

Professional Experience

LDiscovery, LLC (formerly "LegisDiscovery")

Vice President-Electronic Discovery & Forensic Services – March 2005 to present

- Recruited by the founders of LDiscovery to create, equip, staff and supervise their global digital forensics and consulting practice;
- Created digital forensic laboratories in the Philadelphia and Washington, D.C. areas;
- Developed and implemented policies and practices for these facilities in line with ASCLD standards;
- Advise clients on matters involving digital forensics, electronic evidence and electronic discovery needs;
- Oversee and personally conduct forensic acquisitions of electronic evidence, forensic examinations of digital media and conversions of electronic evidence for litigation review; and,
- Provide testimony on matters regarding digital media, electronic evidence, information technology, information security (policy & practice), computer crime, fraud, economic crime and other matters.

Internet Security Systems – Emergency Response Services

Manager-Northeast Region – May 2003 to March 2005

- Recruited by ISS to join their elite Emergency Response Squad;
- Responded at any time, worldwide, to any high-priority computer security incident on systems and networks of any scale

- Conducted investigations in sensitive and potentially hostile environments to protect and recover data, identify malicious network intruders and company insiders responsible for security breaches and data loss, and assess network security stances and incident response readiness of organizations; and,
- Worked with network engineers and penetration testers from ISS and other organizations to harden networks against future attacks, conduct research and test network vulnerabilities to protect clients better.

Teaching and Training

- Lecture Federal, State and Local sworn law enforcement and prosecutors on topics including:
 - digital evidence recovery and analysis;
 - e-mail tracing;
 - information and network security;
 - internet safety for children;
 - internet predators;
 - cyber stalking; and,
 - identity theft and other related topics.
- Helped develop training curriculum for the advanced cyber crime training for prosecutors on behalf of the National District Attorneys Association – case study used in the course is based upon a case I investigated;
- Developed curricula for and lectures at Community College of Philadelphia, Chestnut Hill College of Philadelphia and Carnegie-Mellon University on Digital Forensics, Computer Crime, Electronic Evidence, Computer Security and associated legal issues;
- Co-author of a book on Digital Forensics for Prentice Hall publishers, tentative release in 2008;
- Authored articles and white papers for computer security and investigation trade publications;
- Provide instruction for corporate computer emergency response team personnel (CERTs), IT staff and senior management personnel on incident response methodology, evidence gathering procedures, computer forensic examination techniques and other information security topics;
- Director of Membership for the Philadelphia Chapter of the International Information Systems Forensics Association;
- Technical Editor for the Journal of Information Systems Forensics;
- Consult for the Philadelphia Police Department – Special Victims Unit and Philadelphia District Attorney’s Office and provide ongoing training.

Recent Cases - Expert Analysis, Report, Declaration or Testimony

- Commerce LLC v. Enfield, et al., 1:08-cv-860. (W.D. Mich. 2009) Expert report and testimony regarding forensic analysis at Preliminary Injunction hearing in an Intellectual Property/Departing Employee matter)
-

- Sound Com Corp. v. Rodney Connolly et al., 1:09-cv-1656 (N.D. Ohio July 2009) (Expert report and regarding forensic analysis at Preliminary Injunction hearing in an Intellectual Property/Departing Employee matter)
- Caroline Ways v. Richard Ways, 08-10708 (CCP Montgomery Cty., PA 2009)) (Expert testimony at hearing regarding forensic analysis pertaining to violation of a non-compete agreement as part of a divorce agreement)
- Ameranth v. Marc D. Kessman et al., 1:08-cv-851 (D.DE 2009) (Expert Declaration regarding forensic analysis at Preliminary Injunction hearing in an Intellectual Property/Departing Employee matter)
- Willis of Pennsylvania v. Joseph Kent and Frank Mason, (CCP Delaware Cty., PA 2009)) (Expert report regarding forensic analysis at Preliminary Injunction hearing in an Intellectual Property/Departing Employee matter)
- Formosa Plastics Corp. v. ACE American Insurance Co., 06-cv-5505-HAA-ES (D.NJ 2009) (30(b)(6) expert witness testimony regarding forensic collection and searching of ESI and production of ESI in e-discovery)
- U.S. v. Mohammad Ibrahim Shnewer et al., 07-CR-00459 (D.N.J. 2008) (Expert and fact witness in prosecution of "Fort Dix 6," charge with conspiracy to commit terrorist activities in attempt to destroy Fort Dix, NJ military installation)
- Jacob Stern & Sons, Inc. v. Adele Saviano, Jayant et al., 07-04253 (CCP Montgomery Co., PA 2008) (Expert Declarations regarding forensic analysis at trial in an Intellectual Property/Departing Employee matter)
- Hector Sanchez v. SunGard Availability Services et al., 2:06-cv-03660 DRD-ES (D.N.J 2008) (Expert Declaration regarding forensic analysis in a Title VII matter)
- Synthes (USA) et al. v. Globus Medical, Inc. et al., 04-cv-1235 (E.D. PA 2007) (Expert Report and testimony regarding forensic analysis at trial in an Intellectual Property/Departing Employee matter)
- Murray v. The Honickman Group d/b/a Pepsi et al., BUR-L-001998-07 (Burlington Cty, NJ 2008) (Expert Declarations regarding forensic analysis in Title VII matter)
- Commonwealth v. Jason Johnson, Criminal Matter, CP 51-CR-0000592-2008 (Phila. Cty, PA 2008) (Expert Report for prosecution, leading to guilty pleas, regarding forensic analysis of cell phones in rape prosecutions)
- Commonwealth of PA v. Shirley Gimbel, CP-51-CR-1302009-2006 (CCP Phila. Cty, PA 2008) (Expert and fact witness for prosecution in rape prosecution and conviction)
- Commonwealth of PA v. Michael Kushner, CP-09-CR-0007066-2009 (CCP Bucks Cty, PA 2010) (Expert witness regarding feasibility of defense performing forensic analysis of hard drives at law enforcement laboratory)

Editorial Positions

Editor, HEX – The Collegiate Computer Forensics Journal

Training Provided

National District Attorney's Association - Cyber stalking (Author & Instructor)

National District Attorney's Association - CyberSleuth 1 (Author & Instructor)

National District Attorney's Association - CyberSleuth 2 (Author & Instructor)

National District Attorney's Association – Wired to Fight Fraud (Author & Instructor)
Pennsylvania Office of the Attorney General – Computer Crime: Investigation & Prosecution (Author & Instructor)
Philadelphia (PA) DA's Office – E-mail Tracing & Search Warrants for Electronic Evidence (Author & Instructor)
Philadelphia (PA) DA's Office – Cryptography & Computer Crime (Author & Instructor)
Philadelphia Police Department – Computer Crime/ First Responder's Training (Author & Instructor)
Philadelphia Police Department – E-mail & Internet Investigations (Author & Instructor)
Philadelphia Police Department – Intro to Computer Forensics (Author & Instructor)
Philadelphia Police Department – Interviews & Interrogations of Sex Offenders (Author & Instructor)
Information Systems Security Association – Network Forensic Procedures (Author & Instructor)
Broome County (NY) DA's Office – Electronic & CyberCrime, A to Z (Author & Instructor)
Community College of Philadelphia – Investigating the CyberCrime (Author & Instructor)
Chestnut Hill College – Digital Forensics & Computer Crime (Author & Instructor)
IACIS Advanced Class – Cisco Networking & Forensics for Law Enforcement (Author)
BKForensics – Cell Phone and PDA Forensics

Law Enforcement Career - Philadelphia Police Department

Sergeant: 1st Police District - April to May 2003

- Promoted to rank of Sergeant after placing 9th overall in the City of Philadelphia's written and oral exam based promotional testing process.

Detective: Philadelphia DA's Office – Economic & Cyber Crime Unit - January 2001 to April 2003

- Lead cyber investigator chosen to staff the newly formed District Attorney's Office Cyber Crime Unit.
 - Designed and built the Cyber Crime Unit's laboratory. Constructed the fixed and portable workstations as well as the internal network. Maintained the laboratory, performing routine maintenance of the PC's and network as well as detailed verification procedures on software and hardware tools.
 - Investigated computer crimes of all manner.
 - Drafted and served dozens of search and seizure warrants on various locations. Warrants were for the seizure of computers, electronic evidence and evidence of transactions used to perform e-fraud.
 - Imaged and performed forensic exams on dozens of hard-drives. These examinations were for cases involved various crimes such as forgery, theft of trade secrets, terroristic threats, child exploitation/pornography and extortion.
 - Provided training for prosecutors and detectives on computer crime investigation and court preparation at the Pennsylvania M.P.O.T.E.C. State training facility and National District Attorney's Association.
-

Detective: Special Victims Unit - Child Abuse - December 1999 to January 2001

- Conducted investigations into the injury and exploitation of children. Specialized in cases involving electronic means of exploitation. Assisted the Special Investigations Unit of SVU with cases involving computers and electronic evidence.
- Participated in the drafting and service of dozens of warrants, for both arrest and search and seizure. Seized and processed hundreds of items of evidence, both physical and electronic. Imaged and processed multiple hard drives. Obtained evidence from computers that led to convictions, guilty pleas and property forfeitures by defendants. These convictions, pleas and forfeitures were both in personal cases and the cases of other investigators. Testified in court on numerous occasions regarding aspects of these investigations, seizures and arrests.
- Created a networked MS Access 2000 application that generated a skeletal investigation report for the assigned detective from the information available at the time the incident was initially reported, thereby providing the assigned investigator with more time to investigate an incident. This application also tracked all case and victim data and could be drawn upon for statistics, victim's assistance and caseload tracking information.
- Created a networked MS Access 2000 database application for the input and tracking of overtime usage in the SVU. This application calculated overtime costs and totals, as well as the reason for the overtime. Presently able to generate a weekly, monthly or yearly report that breaks down overtime usage by the unit, squad or individual person who used the time. One officer previously performed this task and it occupied four to six hours per workday, and tracking and graphing overtime usage required a greater expenditure of man-hours. All these overtime tracking tasks now require about fifteen to thirty minutes per day of input, by one officer, and all tracking, reports and graphs are point and click automated.
- All application design and programming completed while carrying a normal caseload assigned unit.
- Provided training to twenty-five newly promoted Philadelphia Detectives on crimes involving computers and their investigation.

Police Office: Center City & 17th Districts - December 1997 to December 1999

- Conducted standard uniform patrol duties both as a foot beat (Center City District) and in a marked unit (17th District). Patrolled high crime & drug areas in the 17th District and business and commercial shopping areas in Center City. Performed hundreds of pedestrian and vehicle investigations and made dozens of arrests for various infractions of the PA Crimes Code. Testified in court regarding arrests.
 - Created an MS Access 2000 application, while a patrol officer in the 17th District, to streamline the duties of the Abandoned Vehicle Officer (AVO) in my District. Before the creation of this program, all forms, reports and records were completed in longhand by the AVO. The application used one set of input data to generate five reports and letters that were needed for each abandoned vehicle. This program also provided a searchable,
-

centralized repository for all of the vehicle data. Shortly after creating this program, all of the AVO's were pulled together in a centralized, citywide Abandoned Vehicle Unit. Deputy Commissioner Thomas Nestel and Chief Inspector Richard Bullick requested that this program to be used on a citywide basis. This application played a pivotal role in a massive urban blight removal program in which the City of Philadelphia removed 1000 abandoned cars per week for 40 weeks. This application has been in full time use, deployed on over 30-networked workstations, processing all of the abandoned vehicle paperwork for the City Of Philadelphia, since February 2000.

Certifications and Targeted Trainings

DFCP (Digital Forensics Certified Professional), CIFI (Certified Information Forensics Investigator), CCE (International Society of Forensic Computer Examiners), TICSA (TruSecure ICSA Certified Security Associate), CHS-III (Certified in Homeland Security, Level 3), Security+ (CompTIA Certified Professional) and ACE (AccessData Certified Examiner) certified. Completed over 400 hours of formal training in forensic data recovery, network security policy and implementation, internet and identity fraud, network intrusion detection, hacker profiling, and the use of related software such as EnCase, ISS Internet Scanner, ISS SiteProtector, Paraben's P-2 technology, SafeBack, Ethereal, Snort, ACID, Access Data's Forensic Toolkit & Password Recovery Toolkit, various forms of proprietary data recovery software, various operating systems such as UNIX & Linux-variants, and related peripherals such as hardware-based write blockers, tape drives, imaging devices & software, and other forms of digital evidence recovery methods and devices.

Training Received

MAGLOCLN - Computers, Crimes & Investigations Seminar
 MAGLOCLN - Advanced Investigation & Data Analysis Techniques Course
 MAGLOCLN - Ilook Computer Forensic Software Training
 MAGLOCLN - Internet Investigations
 MAGLOCLN - Building a Computer Forensics Lab on a budget
 PARABEN - PDA Seizure and Analysis
 NW3C - Basic Data Recovery and Analysis Course
 NW3C - Advanced Data Recovery and Analysis Course
 NW3C - Advanced Data Recovery and Analysis - Internet Trace Evidence Course
 Regional Computer Forensics Group - GMU Computer Forensics Training Symposium 2001
 Access Data - Computer Forensics & Investigations
 International Association of Police Chiefs - Internet Crime and Investigations
 Online Consulting - Advanced Access Programming
 Southern Police Institute - Forensic Interviewing Techniques Course
 Portland State University - Digital Evidence and Computer Crime Issues
 Temple University - Programming Languages
 Temple University - Deductive Logic
 Community College of Philadelphia- Currently pursuing an Associate Degree in Criminal Justice
 Global Knowledge - ISS Introduction to Internet Scanner
 Global Knowledge - ISS Introduction to Site Protector

Global Knowledge – ISS Advanced Site Protector
Global Knowledge – Network Security 1
Global Knowledge – Network Security 2

Professional Affiliations

Pennsylvania Commission on Crime & Delinquency (PCCD) – Committee Member
PCCD Subcommittee on Cyber & Homeland Security - Committee Member
International Association of Computer Forensic Investigators (IACIS)
American College of Forensics Examiners International (ACFEI)
Digital Forensics Certification Board (DFCB)
International Information Systems Forensics Association (IISFA)
International Society of Forensic Computer Examiners (ISFCA)
Information Systems Security Association (ISSA)
High Technology Crime Investigators Association (HTCIA)
High Technology Crime Network (HTCN)
Adjunct Faculty Community College of Philadelphia
Adjunct Faculty Chestnut Hill College

References available upon request